

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Virginia Benda, of the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the FBI for approximately four years and am currently assigned to the Boston Division, Child Exploitation Task Force. While employed by the FBI, I have investigated federal criminal violations related to, among other things, the online sexual exploitation of children. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. In the course of my employment, I have participated in child exploitation investigations involving the possession, distribution, and production of child pornography; and coercion and enticement of minors. I have served as the affiant for and assisted in the execution of federal search warrants.
2. I am currently involved in an investigation regarding violations of 18 U.S.C. §§ 2252A(a)(2)(A) (Distribution of Child Pornography), 2252A(a)(5)(B) (Possession of Child Pornography), and 2423(b) (Travel with intent to engage in illicit sexual conduct), as outlined in the pages that follow.
3. I submit this affidavit in support of an application to search the premises located at 315 Brook Village Road, Apartment #4, Nashua, New Hampshire 03062 (the “SUBJECT PREMISES”), as more fully described in Attachment A, which is incorporated herein by reference; and to seize evidence, instrumentalities, fruits of crime, and contraband as more fully described in Attachment B, which is also incorporated herein by reference.

4. The statements in this affidavit are based in part on information provided by federal agents; written reports about this investigation that I have received, directly or indirectly, from other law enforcement agents; physical surveillance conducted by law enforcement agents; independent investigation and analysis by federal agents/analysts; and my experience, training, and background as a Special Agent with the FBI.
5. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) (Distribution of Child Pornography), 2252A(a)(5)(B) (Possession of Child Pornography), and 2423(b) (Travel with intent to engage in illicit sexual conduct) are located at the SUBJECT PREMISES.

BACKGROUND OF THE INVESTIGATION

6. On or about December 30, 2019, FBI Special Agents and Task Force Officers initiated an operation designed to identify and target adult individuals who were seeking to make contact with and engage in sexually explicit conduct with minors. While working in an undercover capacity, an FBI Online Covert Employee (OCE) was operating a profile on Whisper, a social media application that allows users to post and share photo and video messages anonymously. I have learned the following about Whisper:
 - a. Posts on Whisper – called “whispers” – consist of text superimposed over images, which is a format sometimes referred to as “memes.”
 - b. Whisper allows for individuals to post, meet online, engage in conversation, and exchange photos. Users are not required to provide any personal information or

subscriber information to use the application. Once a user downloads the application to their phone, they are assigned a username and may begin chatting and posting.

- c. Through this application, users can respond to a message with an anonymous public post or privately with a pseudonym via direct message.
 - d. Users do not have a public identity in the application, but do have persistent handles. Users can narrow their search for Whispers within their geographical location, but can only see the general distance between themselves and other users.
 - e. Once two users engage in direct messaging, the conversations are only for those two users to see. Using the direct chat feature allows two users to exchange photos, videos, and text messages. Memes used to originally initiate contact disappear over time or can be taken down by the user who made the post.
7. On December 30, 2019, the OCE observed a post by a user with the username “danglingparticiple” (hereinafter, the SUSPECT WHISPER USER). The post was a meme posted by the SUSPECT WHISPER USER that read something to the effect of “looking for dressing room fun.”¹ The OCE responded to the SUSPECT WHISPER USER’s meme via Whisper’s direct chat feature. The first direct message from the OCE read, “What r u looking for.” The SUSPECT WHISPER USER responded, “Just some sucking and stroking really. More the giving than the getting.” The OCE then asked the SUSPECT WHISPER USER, “What r u into? M? F?” The SUSPECT WHISPER USER replied, “Both. I’d be happy with either.” The OCE then said, “Might have something ur interested

¹ The OCE has preserved the direct messaging between the SUSPECT WHISPER USER and the OCE. However, the original meme either expired or was taken down before it could be captured by the OCE.

in.” The SUSPECT WHISPER USER replied “well let’s see then :)” The OCE then sent a photo of a female FBI special agent kneeling on a bed covered with white sheets. The photo featured the special agent’s body, below the neck, wearing a gray tank top and black shorts.² The SUSPECT WHISPER USER responded, “Oh you could definitely say You’ve got my attention.” The OCE then explained that he was not the one in the picture but that he could make an introduction. The OCE also stated, “Lol I might be too much of a perv for u.” The SUSPECT WHISPER USER responded, “Ha! I highly doubt that. Don’t hold back. Lay it on me.” The OCE then asked, “Lol how do I know ur cool?” The SUSPECT WHISPER USER responded, “I don’t know how to prove I’m cool lol. But I’m into stuff that society would jail me for if I did, so [shrug emoji].” The SUSPECT WHISPER USER then stated, “I fantasize about incest, open family and young. Say about 13+, give or take a couple years depending on looks. Hot is hot, what can I say?”

8. The OCE then asked the SUSPECT WHISPER USER if he was on the messaging application Kik, which is a mobile application that allows users to send each other messages that include text, pictures, and videos. The SUSPECT WHISPER USER said that he was, and the OCE then provided his Kik handle. The SUSPECT WHISPER USER said his Kik handle was “dontusjudgis.” The OCE then immediately received a message on Kik from dontusjudgis (hereinafter, the SUSPECT KIK USER) that read, “hey there.” The SUSPECT WHISPER USER also confirmed on Whisper to the OCE that he messaged

² This photograph has been used in previous investigations; because of the size and figure of the Special Agent, the angle and perspective of the photograph, and the fact that her face is not visible in the image, the photograph has been used by undercover agents to advertise access to a female minor.

him on Kik by sending, “Messaged you.” The chat then switched over to the Kik application.

9. While chatting on Kik, the OCE introduced himself as Mike. The SUSPECT KIK USER then introduced himself as Don. The SUSPECT KIK USER then said, “Glad my interests didn’t scare you away lol.” The OCE responded, “I think our interests are aligned lol.” The SUSPECT KIK USER then said, “Well that’s always a relief to hear. You never know when someone will report you for even just a fantasy. Though mine are fantasies from lack of opportunity lol.” The OCE responded, “Lol I hear ya. Gotta be careful. That’s why I don’t like chatting for long on that Whisper shit.” The SUSPECT KIK USER responded, “Yep. Too sketchy to talk long there. Much better off with Kik or wickr.” The OCE then asked the SUSPECT KIK USER if he was discreet and the SUSPECT KIK USER responded, “Always. I’m married and she doesn’t know I’m on whisper or Kik lol.”
10. The SUSPECT KIK USER then asked the OCE, “And what are you into? Nothing ‘worse’ than what I’m into. I’d find it hard to believe anything could be.” The OCE asked the SUSPECT KIK USER to send him a picture to prove he is not a cop. The SUSPECT KIK USER then sent a photo of what appears to be a man sitting in a black office chair wearing a gray long sleeve t-shirt, and jeans. The man in the picture has a long, unkempt beard, gray and black/brown in color.³
11. The OCE asked the SUSPECT KIK USER to send something a cop wouldn’t send, and the SUSPECT KIK USER suggested that the OCE communicate on Wickr, explaining, “I’ve got stuff no cop would willingly give out to guys of any age and I’ve been banned from

³ As outlined below, the photograph appears to depict DONALD GIBSON.

here before. Wickr would be a good idea.” Wickr Me is an instant messaging application that allows users to exchange end-to-end encrypted and content-expiring messages.

12. The OCE then notified the SUSPECT KIK USER that he downloaded the Wickr Me application. The SUSPECT KIK USER then wrote, “Where are you right now? Home? I don’t want you opening this where you’ll get in trouble.” When the OCE responded that he was at work, the SUSPECT KIK USER responded, “Ok. Definitely hide in the bathroom or something. Or just make damn sure no one is around and you’re not on works WiFi.”
13. The OCE then received a message on the Wickr Me application from a user named “olivetanday” (hereinafter, the SUSPECT WICKR USER). The OCE asked the SUSPECT KIK USER “Who is olivetanday?” The SUSPECT KIK USER then explained that it was him and that “Olive = ‘I love’ Tanday = ‘T and A’ lol.” The SUSPECT WICKR USER then sent the OCE two images. The first image portrayed a female child who appeared to be approximately four to six years old breastfeeding from a nude adult female. This image disappeared from the chat before it was captured for evidence. The second image portrays a female child who appears to be approximately five to seven years old, performing oral sex on an adult male.⁴ The OCE then received a message from the SUSPECT KIK USER that said, “Not a cop. So go ahead and tell me.”
14. On December 30, 2019 the OCE then told the SUSPECT KIK USER that the picture of the female FBI special agent he sent on Whisper was his daughter. The SUSPECT KIK USER then replied, “Then you’re a lucky guy. She’s definitely got an amazing figure. It would take everything I’ve got to not fuck her if I was you. Unless she wanted to and then I’d

⁴ This image is available for the Court’s review.

absolutely fuck her constantly...I'd be jerking off to her all the time and trying to catch her naked as often as possible." The SUSPECT KIK USER then inquired, "You said you could introduce me but I'm [*sic*] the extremely unlikely event that happened, would she be down to fuck? If she was, would you join? *in the."

15. During their conversation on Kik, the OCE told the SUSPECT KIK USER that his daughter was 13 years old and the SUSPECT KIK USER responded, "That's old enough in my book! Makes me want to keep looking at that picture."

Distribution of Child Pornography

16. On or about January 19, 2020 the SUSPECT KIK USER told the OCE that he was going to send him videos on Wickr. Shortly thereafter, the OCE received approximately 17 videos from the SUSPECT WICKR USER. Out of the approximate 17 videos sent, 15 portray what I believe to be child pornography, including female children who appear to be between the ages of five and 14 years of age, nude, masturbating, engaging in vaginal and oral sex, blindfolded, bound, or engaged in bestiality. One of the videos is described below:

- a. Filename beginning with "*trim.55B31028-91F9-451D-A*": This video, approximately 45 seconds in length, depicts a female child who appears to be approximately four to six years old performing oral sex on an adult male. During the course of the video, the child pulls down her shorts, revealing her vagina. The child is then instructed to turn around by whoever is filming. The child then bends over and spreads her buttocks for the camera, focusing on her anus and vagina.⁵

⁵ A still shot from this video is available for the Court's review.

17. On or about January 23, 2020, the OCE received approximately 10 videos from the SUSPECT WICKR USER, approximately eight of which consist of what I believe to be child pornography. One of the videos is described as follows:
 - a. Filename *2014-04-15_22-26-50_50_986.-1*: This video is approximately 17 minutes in length. It depicts a female child who appears to be approximately four to six years old, nude in a bedroom with a nude adult female and nude adult male. A collar with leash attached is placed around the child's neck and the child begins to cry. She is laid down on the bed while the adult female digitally penetrates her and performs oral sex on her. An adult penis is being masturbated in the frame. The adult male then attempts to penetrate the child from behind while the adult female holds the child's buttocks in place.⁶
18. On or about January 24, 2020, the OCE received approximately three videos that portray what I believe to be child pornography from the SUSPECT WICKR USER. One of the videos is described as follows:
 - a. Filename *video11-1*: This video is approximately 40 seconds in length. It depicts a female child who appears to be approximately eight to 11 years old, wearing a mask, with her breasts and vagina displayed. A white canine then climbs on top of the child and appears to penetrate the child's vagina with his penis.⁷
19. During the chats on Kik, the SUSPECT KIK USER sent child pornography to the OCE on Wickr sometimes late at night after revealing that he was home. The SUSPECT KIK USER also told the OCE that he has an extensive collection of videos he was trying to organize

⁶ A still shot from this video is available for the Court's review.

⁷ A still shot from this video is available for the Court's review.

while at home and that he would bring the OCE a thumb drive with his collection when they met in person to perform illicit sexual acts with the OCE's 13 year old daughter.

Travel with Intent to Engage in Illicit Sexual Conduct

20. On January 27, 2020, the OCE told the SUSPECT KIK USER that he spent the previous weekend with his daughter. After the SUSPECT KIK USER asked how the weekend went, the OCE replied, "It was a lot of the previous weekend but just MORE of it. Lol. With her initiating some of the time which I think is a really good sign?" The OCE then told the SUSPECT KIK USER that he mentioned the SUSPECT KIK USER to his daughter and that she seemed open to the idea of getting the SUSPECT KIK USER involved in a sexual encounter. The SUSPECT KIK USER replied, "Man if she is I would be over the moon ecstatic! I won't get my hopes up though and of course I'd want her to be sure, you know?" The OCE and the SUSPECT KIK USER then began discussing logistics of meeting in person for the sexual encounter with the OCE's daughter.
21. The SUSPECT KIK USER wrote, "Yeah we can meet just the two of us however you'd like to arrange it." The OCE suggested, "Even if Amy stayed up in the room and I met u in the lobby or something. Just to make sure ur not some crazy killer lol. If u are at least Amy will be safe and only I will get killed lol." The SUSPECT KIK USER then responded, "Yeah for sure. Then if you wanted to call it off I could drive off and that would be that. Lol definitely not a killer. I swear on my own life! I'm happy to do whatever it takes, you know? I don't want to mess anything up." In the course of the conversation, the SUSPECT KIK USER said, "It would have to be during the work week of course. Unless we did wait for golf weather.....Well as long as you can pull her from school without her mom finding out, or unless you've got that point covered we could really do it anytime. Though I would

say that next week and on would work for me. This week is swamped with work and home life.”

22. The OCE then told the SUSPECT KIK USER that his daughter had a doctor’s appointment the following week. The SUSPECT KIK USER replied, “Oh man that would be perfect!.....Morning would be perfect. Give us plenty of time after then.” The OCE then suggested getting food in the hotel room and SUSPECT KIK USER responded that he would contribute money toward the food and pay for half the room and said, “And if she ends up being down for this I will definitely bring condoms as agreed. And you can bring some too if you don’t trust me to remember. But we definitely don’t need her getting pregnant even if she is on BC. That stuff does fail on occasion.”
23. Over several conversations, the OCE and the SUSPECT KIK USER planned to meet at a hotel in Massachusetts so that they could have sexual contact with the OCE’s 13 year old daughter. The OCE identified a specific hotel in Tewksbury, Massachusetts. In a conversation on February 3, 2020, the OCE told the SUSPECT KIK USER that he could reserve a room on the evening of February 4, 2020 so that it would be available to them in the morning of February 5, 2020, and indicated that they could request a late check-out. The SUSPECT KIK USER told the OCE that his wife thinks he is working on February 5, 2020, so she would not expect him home until around 4:00 p.m. The SUSPECT KIK USER further asked the OCE about his daughter’s excitement, enthusiasm, and sex drive level and asked, “Are you going to be ok with seeing her and I together? Does it make you nervous thinking about it?” In earlier conversations, the SUSPECT KIK USER had told the OCE that he wanted her to perform oral sex on him, and that he wanted to digitally penetrate her, perform oral sex on her, and have sexual intercourse with her.

Identification of the Suspect User

24. In the course of the chat, the SUSPECT KIK USER told the OCE that he lives in Nashua, New Hampshire and works in Bedford, New Hampshire in the planning office for a machine shop of an international company. The FBI identified a company called Ferrotec Corporation, located at 33 Constitution Drive in Bedford, New Hampshire with an international headquarters outside of the United States.
25. An open-source Internet search located a DONALD GIBSON employed at Ferrotec. A commercial database search using Accurant identified only one DONALD GIBSON currently located in Nashua, NH, and showed him to be associated with the SUBJECT PREMISES.
26. A search of records held by the New Hampshire Registry of Motor Vehicles for DONALD GIBSON located driver's license information including a photograph of DONALD GIBSON and the SUBJECT PREMISES listed as his address.
27. A commercial database search using Accurant for additional individuals associated with the SUBJECT PREMISES identified KELSEY GIBSON as a resident. Records held by the New Hampshire Registry of Motor Vehicles show the following vehicles being registered to KELSEY GIBSON:
 - a. 2002 black Nissan Pathfinder, expired New Hampshire license plate 336 5086
 - b. 2014 black Chevrolet Traverse, New Hampshire license plate 450 7625
 - c. 2004 red Honda Accord, New Hampshire license plate 358 0527
28. On January 27, 2020 the SUSPECT KIK USER informed the OCE that he currently drives a Chevrolet Traverse and used to have a Nissan Pathfinder. On both January 22 and 23, 2020, agents observed a black Chevrolet Traverse with New Hampshire license plate 450

7625 parked at Ferrotec. On January 27, 2020 the same Chevrolet Traverse was observed parked at the SUBJECT PREMISES.

29. Throughout the chats on Kik, the SUSPECT KIK USER told the OCE that he had three children under the age of six – two sons and one daughter. Social Media research revealed that DONALD GIBSON and KELSEY GIBSON both have individual Facebook accounts. Featured in both Facebook accounts is a white male with a long gray and brown/black unkempt beard. The male pictured appears to be the same male pictured in DONALD GIBSON's driver's license photograph and in the photograph sent to the OCE by the SUSPECT KIK USER, as described above. Also featured within both Facebook accounts are photographs of the same three children who appear to match the ages and genders of the children described by the SUSPECT KIK USER.
30. On January 8, 2020, the SUSPECT KIK USER told the OCE that his daughter turned five years old that day, that he got her a Polly Pocket as a gift, and that they planned on celebrating the birthday the following day. On January 8, 2020, KELSEY GIBSON posted on her Facebook page that her daughter turned five years old that day, and the following day, posted birthday party photographs showing her daughter holding a newly unwrapped Polly Pocket doll.
31. On January 15, 2020 the SUSPECT KIK USER told the OCE that it was his oldest son's birthday that day. The SUSPECT KIK USER told OCE that his oldest son is now six years old, his daughter is five, and his youngest son is three but will be four in April. On that same day, KELSEY GIBSON posted on her Facebook account that her son turned six years old that day.

32. Based on all of the foregoing, I submit that there is probable cause to believe that DONALD GIBSON is the SUSPECT WHISPER USER, the SUSPECT KIK USER, and the SUSPECT WICKR USER.

CHARACTERISTICS COMMON TO CONSUMERS OF CHILD PORNOGRAPHY

33. Based on my previous training and experience related to investigations involving child pornography and the sexual abuse of children, I have learned that individuals who create, possess, receive, distribute, or access with intent to view child pornography (collectively, “consumers” of child pornography) have a sexual interest in children and in images of children. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to such consumers of child pornography, as outlined in the following paragraphs.
34. The majority of consumers of child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.
35. Consumers of child pornography may collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics, or digital or other images for their own sexual gratification. These individuals often also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors are often found on computers and digital storage devices that also contain child pornography, or that are used to communicate with others about sexual activity or interest in children. Such

images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.

36. Many consumers of child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They regularly maintain their collections in the privacy and security of their homes, cars, garages, sheds, or other secure storage location, such as on their person.
37. Some consumers of child pornography have also been found to download, view, and then delete child pornography on a cyclical and repetitive basis in an attempt to destroy evidence and evade law enforcement. I know through my training and experience that this type of behavior is often seen in individuals who have some level of technical expertise, are aware of law enforcement efforts to investigate child pornography offenses, gain access to child pornography on anonymized dark web networks like Tor (which is sometimes perceived by offenders as being “safe” from law enforcement detection), or struggle with their addiction or attraction to child pornography.
38. Consumers of child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. Furthermore, individuals who would have knowledge about how to access a hidden and embedded chat site would have gained knowledge of its location through online

communication with others of similar interest. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, e-mail, bulletin boards, chat sites, web forums, instant messaging applications, and other similar vehicles of communication.

39. Consumers of child pornography often collect, read, copy, or maintain names, screen names or nicknames, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium from which they were derived, in written hardcopy, on computer storage devices, or merely on scraps of paper.
40. As referenced below, based on my training, knowledge, experience, and conversations with others in law enforcement, I understand that an individual who possesses images and/or videos depicting child pornography on one type of digital media and/or online communication or storage account is likely to possess child pornography on additional types of digital media or online communication or storage accounts that he possesses or controls. Additionally, based on this training and experience, I understand that an individual who discusses the sexual abuse or exploitation of children through one digital medium is likely to conduct those communications through additional digital media to which he has access or control.
41. Based on all of the foregoing, including the fact that he distributed child pornography to the OCE and has made plans to travel from New Hampshire to Massachusetts to meet the OCE in person to engage in sexual conduct with the OCE's 13 year old daughter, I submit

that DONALD GIBSON is likely to exhibit characteristics common to consumers of child pornography.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

42. I have had training and experience in the investigation of computer-related crimes, including those involving child pornography. Based on my training and experience, I know the following:
- a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
 - b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.
 - c. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged

into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person

- d. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
- e. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Google, Yahoo!, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.
- f. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of

an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

43. As described above and in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).
44. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, accessing the internet, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.
45. I am aware of a report from the United States Census Bureau that shows that in 2016, among all households nationally, 89 percent had a computer, which includes smartphones, and 81 percent had a broadband Internet subscription. Specifically, in 2016, when the use

of smartphone ownership was measured separately for the first time, 76 percent of households had a smartphone and 58 percent of households had a tablet, and 77 percent of households had a desktop or laptop computer. Further, according to the Pew Research Center, as of 2019, 96 percent of adult Americans own a cellphone, and 81 percent own a cellphone with significant computing capability (a “smartphone”). The percentage of adults that own a smartphone is even higher among younger demographic groups: 96 percent of 18-29 year olds, 92 percent of 30-49 year olds, and 79 percent of 50-64 year olds owned smartphones in 2019.

46. I submit that if a computer or storage medium is found in the place to be searched, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the reasons that follow.
47. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.
48. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

49. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.
50. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” An internet browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.
51. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:
 - a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail

programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity

associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

52. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
53. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
54. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
55. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or

received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

56. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

- a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.
- b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert

possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

57. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.
58. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B. If however, the law enforcement agents cannot make a determination as to use or ownership regarding any

particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.


59. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.
60. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CONCLUSION

61. Based on the foregoing, I submit there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES as described in Attachment A, authorizing the seizure and search of the items described in Attachment B.


/s/ Virginia Brenda _____
Virginia Benda
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 5th day of February, 2020.



HONORABLE
United States Magistrate Judge

I have reviewed the images referenced in Paragraphs 13, 16, 17, and 18 above and I find probable cause to believe that they depict minors engaged in sexually explicit conduct. The affiant shall preserve the images provided to the Court for the duration of the pendency of this matter, including any relevant appeal process.



HONORABLE
United States Magistrate Judge

**ATTACHMENT A
PROPERTY TO BE SEARCHED**

The SUBJECT PREMISES is the residence located at 315 Brook Village Road, Apartment #4, Nashua, New Hampshire 03062. The SUBJECT PREMISES is one of four units making up the structure numbered 315. The structure numbered 315 is a two story structure, beige and brown in color with white trim. It is part of similar structures that make up the expansive community at Brook Village Road. It is pictured below:





ATTACHMENT B
ITEMS TO BE SEIZED AND SEARCHED

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (Distribution of Child Pornography), 2252A(a)(5)(B) (Possession of Child Pornography), and 2423(b) (Travel with intent to engage in illicit sexual conduct), including:
 - A. Records and tangible objects pertaining to the following topics:
 1. Images or visual depictions of child pornography;
 2. Child erotica, including text, images, and visual depictions;
 3. Communications about child pornography or sexual activity with or sexual interest in minors;
 4. Internet activity reflecting a sexual interest in minors or child pornography;
 5. Information concerning the minor subject of any visual depiction of child pornography, child erotica, sexual activity with other minors or adults, or of sexual interest, or that may be helpful in identifying any such minor;
 6. Address books (virtual and physical), names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of committing violations of the subject offenses;
 7. Membership in online groups, clubs, or services that provide, make accessible, or otherwise concern child pornography; and
 8. The existence of e-mail accounts, online storage, or other remote computer storage.
 - B. Records and tangible objects pertaining to the existence, identity, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;
 - C. Records and tangible objects relating to the ownership, occupancy, or use of the premises to be searched (such as utility bills, phone bills, rent/mortgage payments,

photographs, insurance documentation, receipts, and check registers);

- D. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant (“the computer equipment”):
1. evidence of who used, owned, or controlled the computer equipment;
 2. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;
 3. evidence of the attachment of other computer hardware or storage media;
 4. evidence of counter-forensic programs (and associated data) that are designed to eliminate data;
 5. evidence of how and when the computer equipment was used or accessed;
 6. records of or information about any Internet Protocol addresses used;
 7. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;
 8. contextual information necessary to understand the evidence described in this attachment;
 9. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage; and

- II. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for the items described in Paragraph I.

DEFINITIONS

For the purpose of this warrant:

- A. “Computer equipment” means any computer hardware, computer software, mobile phone, storage media, and data.
- B. “Computer hardware” means any electronic device capable of data processing (such as a computer, smartphone, cell/mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor,

and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds, or symbols.
- G. "Child Pornography," as defined in 18 U.S.C. § 2256(8)(A), means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.
- H. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions; this also includes texts or discussions regarding minors engaged in sexual acts or conduct.

EXECUTION

Searching agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence authorized by this warrant, as outlined above. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents may make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary.